REMARKS

Claims 1-24 remain in the application. Claims 22-24 are newly added. Applicant respectfully requests re-examination.

The Office Action rejected claim 14 as being anticipated by *Benaloh* (U.S. 6,886,098). Applicant respectfully traverses.

Benaloh is a reference that seeks to reduce the number of keys required to ensure secure content delivery. It reduces the number of keys to be distributed from m*r keys to m keys where m is the number of customers and r is the rights obtained by the customers. It associates a small odd prime integer (p_i) with each data to be protected. No prime is associated more than one data, and the set of these primes and their association is completely public. The owner of the data selects two large prime integers and forms their product (N). The owner of the data also selects a random base integer value (x). A reference value (y) may then be formed as the random base integer value (x) raised modulo N to the power of the product of all small primes associated with the data. This reference (y) can be made public. The content key used to encrypt each data to be secured is a fixed function of the path root modulo N of the reference integer value (y), where p is the small odd prime integer. Each user is then given x to the power m, modulo N, of the product of all primes which are associated with data to which the user is not entitled. From this single value, a user can easily compute the content key for all the data to which the user is entitled. However, a user cannot obtain any content keys corresponding to data to which the user is not entitled. Furthermore, no group of users can conspire to obtain access to any content keys to which none of the participants have individual access. (Col. 1, ln. 40 – Col. 2, ln. 37).

The present invention seeks to solve the problem of carrying a heavy but delicate delivery device while maintaining adequate security for the delivered data content. It accomplishes this

by using a semi-permanently installed Terminal Data Loader ("TDL") along with a transportable cryptographically secure media element. (Specification ¶¶ 0006-0007). In one embodiment, as shown in Figure 2, the TDL comprises a media unit 102, a control processor unit 108, a security processor unit 204, a physical key unit 208, and a wireline communication unit 112. The media unit 102 receives a removable, transportable media element 104 that contains encrypted media data. The media unit 102 reads the encrypted media data and transmits an encrypted media signal 202 to the security processor unit 204. The control processor unit 108 interfaces with a physical key unit 208 that receives a physical key 212. The physical key unit 208 produces encryption and decryption key information 210 using physical key 212. The encryption and decryption key information 210 is passed to the security processor unit 204. The security processor unit 204 produces an unencrypted media signal 206 from the encrypted medial signal 202 using the encryption and decryption key information 210. The unencrypted media signal 206 is passed to the control processor unit 108 which produces an information signal 110. To produce the information signal 110, the control processor unit 108 can parse the unencrypted medial signal 206 into blocks of a predetermined size to facilitate the use of block-cipher protocols as well as to limit the bandwidth required for transfers in the presence of other network devices. The wireline communication unit 112 can receive an information signal 110 and output a wireline signal 114 to a mobile platform network 116. (¶¶ 0028 – 0033; Fig. 2).

Benaloh does not teach or suggest "creating delivery blocks," "encrypting delivery blocks," "writing delivery blocks," "decrypting delivery blocks," "collecting delivery blocks" or "reassembling delivery blocks." *Benaloh* does not use delivery blocks. *Benaloh* only splits the movies into sections based on cinematic content. For example, the database 1406 is logically divided into eight segments 1412-1426 with the first version of the movie 1408 comprising

segments 1412, 1416, 1420, and 1424 and the second version of the movie 1410 comprising segments 1414, 1418, 1422, and 1426. Although there are eight total segments, only four segments are needed to view the entire movie. Therefore, there are sixteen combinations of segments that will render a complete movie. (Col. 13, lns. 15-51; Fig. 4). Thus, the decision on where and how to split the movie is not based on any delivery or efficiency concerns, but rather on cinematic concerns.

In contrast, in the present invention, the unencrypted medial signal 206 can be parsed into delivery blocks of a predetermined size. The predetermined size can be chosen to facilitate the use of block-cipher protocols. Furthermore, parsing can be done to limit the bandwidth required for transfers in the presence of other network devices. (¶ 0033). Thus, rather than parsing based on cinematic concerns to produce different versions of a movie, the present invention parses the unencrypted medial signal to create delivery blocks of a predetermined sized based on efficiency concerns.

Applicant respectfully requests that this rejection be withdrawn.

The Office Action rejected claims 1-6, 8, 16-17, and 19-20 under 35 U.S.C. §103(a) as being unpatentable over *Mitchell* (U.S. 6,741,841). Applicant respectfully traverses.

Mitchell is directed towards a communication system for a mobile platform. The communication system includes a wireless docking area transceiver, a wireless platform transceiver, and a storage unit. The storage unit is located on the mobile platform. The wireless docking area transceiver provides video data to the wireless platform transceiver while the mobile platform is at the docking area. The storage unit stores the video data for playback in the mobile platform. (Col. 3, ln. 64 – ln. 6).

With respect to claim 1, *Mitchell* does not teach or suggest "a media unit operatively connectable to a transportable media element containing media data, the media unit being capable of reading the media data from the media element and outputting a media signal." The Office Action cited to the storage unit 52 as being the media unit. However, at best, storage unit 52 is possibly a media element, not a storage unit. Storage unit 52 "can include stored video data and audio data" it can alternatively be "an on-board source, such as, video discs or video tapes" or a "disc drive capital or magnetic, a tape drive, or other apparatus capable of storing video data or signals." Storage unit 52 only stores video data or signals, it does not read the media data from the media element, nor is there any indication that it outputs a media signal as a result of reading the media data.

Mitchell also does not teach or suggest "a control processor unit for receiving the media signal from the media unit and outputting an information signal." The Office Action cited to a communication unit comprising a receiver 50, network 54, and a storage unit 52 for receiving the information signal and outputting a signal to a network. The Office Action also cited to network 54 as being computer based and thus necessarily containing a control processor unit. However, the communication unit is not the control processor unit. The control processor unit in Mitchell is contained within the network 54, which is part of the communication unit. Network 54 is also not the control processor unit since it may contain the control processor unit within it.

Furthermore, while Network 54 may be computer based and may contain a control processor unit, there is no indication as to what the control processor unit within Network 54 does or how it functions. *Mitchell* does not disclose if the control processor unit within Network 54 receives a media signal from the media unit or if it even outputs an information signal. This is especially true considering that there is no indication that Network 54 itself receives a media

signal from the media unit or that it outputs an information signal. If Network 54 does not receive a media signal from the media unit it would be difficult for the control processing unit to receive a media signal from the media unit. Likewise if network 54 does not output an information signal, it would be difficult from the control processing unit to output an information signal.

Applicant respectfully requests that this rejection be withdrawn.

Claims 2-6 depend from and further limit claim 1 and are patentable for at least the reasons given above.

Claim 8, depends from and further defines claim 1 and is patentable for at least the reasons given above. *Mitchell* also does not teach or suggest "wherein the media element can be safely used on the mobile platform without requiring a mobile platform precertification of the media element against harmful interactions with the mobile platform." The Office Action cited to programming other than television programming such as Internet services as the media element that can be safely used on the mobile platform with require a mobile platform precertification of the media element against harmful interactions with the mobile platform. However, programming other than television programming does not disclose the media element in which they are contained. Furthermore, if Internet services are utilized, especially if they are transmitted wirelessly, this could potentially cause harmful interactions with the mobile platform. In addition, *Mitchell* does not indicate that the medium that the Internet services are provided must be precertified against harmful interactions with the mobile platform.

Applicant respectfully requests that this rejection be withdrawn.

All arguments for patentability with respect to claim 1 is repeated and reincorporated herein for claims 16-17, and 19-20.

Furthermore, with respect to claim 19, *Mitchell* does not teach or suggest "writing the media signal to the transportable media element with the media unit so that the transportable media element contains media data corresponding to the media signal." Mitchell only discloses wirelessly transferring aircraft data from the aircraft 120 via gatelink 130. Thereafter, the aircraft data may be transferred to mass memory storage unit 119. Mobile platform 35 can be an aircraft such as aircraft 120. (Col. 6, lns. 38-42; Fig. 1, 7). However, as seen in Figures 1 and 7, mass memory storage unit 119 does not reside in aircraft 120 and thus, is not part of the mobile platform 35. Therefore, *Mitchell* does not disclose writing the medial signal to the transportable medial element.

Applicant respectfully requests that this rejection be withdrawn.

The Office Action rejected claim 7 under 35 U.S.C. §103(a) as being unpatentable over *Mitchell* in view of *Chan* (U.S. 6,775,087). Applicant respectfully traverses.

Since claim 7 depends from and further narrows claim 1, it is patentable for at least the same reasons. Applicant respectfully requests that this rejection be withdrawn.

The Office Action rejected claims 9-10, 15, 18, and 21 under 35 U.S.C. §103(a) as being unpatentable over *Mitchell* in view of *Benaloh.*

With respect to claim 9, the Office Action admits that *Mitchell* does not disclose "a security processor unit for receiving an encrypted media signal and outputting an unencrypted media signal based on one or more predetermined cryptographic keys and utilizing a predetermined cryptographic algorithm" or a "a physical key unit for receiving a physical key, the physical key unit and physical key for determining at least one cryptographic key."

Benaloh does not disclose "a security processor unit for receiving an encrypted media signal and outputting an unencrypted media signal based on one or more predetermined

cryptographic keys and utilizing a predetermined cryptographic algorithm" or a "a physical key unit for receiving a physical key, the physical key unit and physical key for determining at least one cryptographic key." *Benaloh* only discloses that the player 200 requires a content key 302 to decrypt/play an encrypted movie and uses 1.) a public key 308 and private key 310 of key loading pair 308 and 2.) a public key 314 and private key 316 of device key 312 to receive the content key. (Co. 6, ln. 23 – Col. 7, ln. 12). However, there is no indication of what part of the player 200 receives the content key or any of the other public and private keys. Furthermore, there is no indication of what part of the player 200 receives the encrypted media signal and outputs an unencrypted media signal.

In contrast, in the present invention, the control processor unit 108 interfaces with a physical key unit 208 that receives a physical key 212. The physical key unit 208 produces encryption and decryption key information 210 using physical key 212. The encryption and decryption key information 210 is passed to the security processor unit 204. The security processor unit 204 produces an unencrypted media signal 206 from the encrypted medial signal 202 using the encryption and decryption key information 210. (Specification ¶¶ 0028 – 0031; Fig. 2).

Claim 10 further defines and narrows claim 9 and is patentable for the same reasons.

For claim 15 the arguments for patentability with respect to claim 9 is repeated and incorporated herein.

Furthermore, *Benaloh* does not teach or suggest "collecting the decrypted media signal into delivery blocks of a predetermined size." *Benaloh* does not use delivery blocks. *Benaloh* only splits the movies into sections based on cinematic content. For example, the database 1406 is logically divided into eight segments 1412-1426 with the first version of the movie 1408

comprising segments 1412, 1416, 1420, and 1424 and the second version of the movie 1410 comprising segments 1414, 1418, 1422, and 1426. Although there are eight total segments, only four segments are needed to view the entire movie. Therefore, there are sixteen combinations of segments that will render a complete movie. (Col. 13, lns. 15-51; Fig. 4). Thus, the decision on where and how to split the movie is not based on any delivery or efficiency concerns, but rather on cinematic concerns.

In contrast, in the present invention, the unencrypted medial signal 206 can be parsed into delivery blocks of a predetermined size. The predetermined size can be chosen to facilitate the use of block-cipher protocols. Furthermore, parsing can be done to limit the bandwidth required for transfers in the presence of other network devices. (¶ 0033). Thus, rather than parsing based on cinematic concerns to produce different versions of a movie, the present invention parses the unencrypted medial signal to create delivery blocks of a predetermined sized based on efficiency concerns.

For claim 18 the arguments for patentability with respect to claim 9 is repeated and incorporated herein. Applicant requests that the rejection be withdrawn.

For claim 21, the arguments for patentability with respect to claim 9 is repeated and incorporated herein.

Furthermore, *Mitchell* does not teach or suggest "writing the media signal to the transportable media element with the media unit so that the transportable media element contains media data corresponding to the media signal." Mitchell only discloses wirelessly transferring aircraft data from the aircraft 120 via gatelink 130. Thereafter, the aircraft data may be transferred to mass memory storage unit 119. Mobile platform 35 can be an aircraft such as aircraft 120. (Col. 6, lns. 38-42; Fig. 1, 7). However, as seen in Figures 1 and 7, mass memory

storage unit 119 does not reside in aircraft 120 and thus, is not part of the mobile platform 35. Therefore, *Mitchell* does not disclose writing the medial signal to the transportable medial element.

Applicant requests that this rejection be withdrawn.

The Office Action rejected claims 11-13 under 35 U.S.C. §103(a) as being unpatentable over *Mitchell* in view of *Benaloh* and *Schneier* ("Applied cryptography second edition"). Applicant respectfully traverses.

Claims 11-13 depend from and further limit the scope of claim 1. Claims 11-13 are seen as patentable for at least the reasons given above for the patentability of claim 1.

Applicant requests that this rejection be withdrawn.

As for newly admitted claims 22-23, the Office Action admits that Mitchell does not disclose "a wireline communication unit for receiving the information signal and outputting a wireline signal to a network on the mobile platform" in claim 1. However, even if an in-flight video system uses a wire to carry a video signal to the passenger display unit, there is no indication as to which type of wireline communication unit would be used.

Furthermore, for claim 24, the wireline communication unit does not use a wire, but rather is wireless.

In light of the above amendments and remarks, applicant believes that all the examined claims remaining in the application are allowable and respectfully requests an early indication of same.

I hereby certify that this correspondence is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on May 8, 2007.

Express Mail Label No.: EV 821164797 US

By: Heather Schnabel

Heather Schnabel
Signature

Dated: May 8, 2007

Very truly yours,

SNELL & WILMER L.L.P.

Albin H. Gess
Registration No. 25,726
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626
Telephone: (714) 427-7020
Facsimile: (714) 427-7799